UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION AT COLUMBUS

SUSAN WARDLE-BURKE, individually and on behalf of all others similarly situated,
% Dann Law
15000 Madison Avenue
Lakewood, OH 44107

Plaintiff,

v.

VICTORIA'S SECRET & CO.
% CT Corporation System, Reg. Agent
4400 Easton Commons Way, Suite 125
Columbus, OH 43219

and

VICTORIA'S SECRET STORES, LLC
% CT Corporation System, Reg. Agent
4400 Easton Commons Way, Suite 125
Columbus, OH 43219

Defendants.

Case No.

Judge

Magistrate Judge

CLASS ACTION COMPLAINT FOR DAMAGES
(With Jury Endorsed Hereon)

Plaintiff Susan Wardle-Burke, individually and on behalf of all others similarly situated ("Plaintiff"), through counsel, brings this Class Action Complaint for Damages against Defendants Victoria's Secret & Co. and Victoria's Secret Stores, LLC ("Defendants"). Plaintiff makes these allegations with personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated customers' names, dates of birth,

Social Security numbers, driver's license numbers, state identification numbers, passport numbers, financial account information, digital signatures, medical information, health insurance information, biometric information, and mother's maiden names (the "PII") from hackers.

2. Defendants' data security fails allowed a targeted cyberattack to compromise Defendants' networks (the "Data Breach"), that, upon information and belief contained the PII of the Plaintiff and other individuals ("the Class"). The Data Breach occurred on or about May 27, 2025 and as of the filing of this Complaint, Defendants have not begun to send out notices to affected individuals.[1]

3. Defendant Victoria's Secret & Co is a specialty retailer of modern, fashion-inspired collections including lingerie, athleisure, swimwear, as well as fragrances and body-care.[2]

4. Defendant Victoria's Secret Stores LLC is an LLC which operates and maintains Defendants' retail locations.

5. Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' PII with which it was entrusted for either treatment or employment, or both.

6. Upon information and belief, Defendants breached their duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on

[1] "Victoria's Secret's Website Offline Following a Cyberattack." https://securityaffairs.com/178432/hacking/victorias-secrets-website-offline-following-a-cyberattack.html (last visited May 29, 2025); *see also* "Victoria's Secret takes down website after 'security incident'", https://www.nbcnews.com/tech/security/victorias-secret-takes-website-security-incident-rcna209682 (last visited May 29, 2025).

[2] *See* https://www.victoriassecretandco.com/our-company/about-us (last visited May 28, 2025).

data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class members of Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

7. Defendants impliedly understood their obligations and promised to safeguard Plaintiff's and Class members' PII. Plaintiff and Class members relied on these implied promises when seeking out and paying for Defendants' services. But for this mutual understanding, Plaintiff and Class members would not have provided Defendants with their PII. Defendants, however, did not meet these reasonable expectations, causing Plaintiff and Class members to suffer injury.

8. Defendants disregarded the rights of Plaintiff and Class members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class members with prompt and full notice of the Data Breach.

9. In addition, Defendants failed to properly monitor the computer network and systems that housed the PII. Had they properly monitored their property, they would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the PII of Plaintiff and Class members.

10. Plaintiff's and Class members' identities are now at risk because of Defendants' negligent conduct since the PII that Defendants collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiff and Class members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendants' unreasonable and inadequate data security practices, Plaintiff and Class members have suffered numerous actual and concrete injuries and damages.

12. Plaintiff and Class members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

13. Plaintiff and Class members have suffered or may suffer numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs should identity theft occur; (d) loss of time incurred should identity theft occur; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect it.

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose PII was stolen during the Data Breach.

15. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct and asserting claims for: (i) negligence and negligence per se, (ii) breach of implied contract, (iii) breach of fiduciary duty, (iv) unjust enrichment, and (vi) declaratory relief.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendants, and declaratory relief.

17. The exposure of one's PII to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's PII was private. Not anymore. Now, their PII is forever exposed and unsecure.

PARTIES, JURISDICTION AND VENUE

18. Plaintiff Susan Wardle-Burke is an adult individual who at all relevant times has been a citizen and resident of Austintown, Ohio.

19. Defendant Victoria's Secret & Co was, at the time this action was filed, and continues to be a corporation incorporated under the laws of the State of Delaware, with its principal place of business in Reynoldsburg, Ohio.

20. Defendant Victoria's Secret Stores, LLC was, at the time this action was filed, and continues to be a limited liability company incorporated under the laws of the State of Delaware, with its principal place of business in Reynoldsburg, Ohio.

21. The Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this case is brought as a class action, Plaintiff and Defendants are diverse parties, more than 100

members are in the putative class, and the amount in controversy exceeds $5 million.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and the Defendants have harmed Class members residing in this District.

GENERAL FACTUAL ALLEGATIONS

Defendants Business Practices

23. Defendants represent to their customers and the public that they possesses robust security features to protect PII. Defendants' privacy policy specifically states that they take steps to keep PII secure. The policy[3] provides in relevant part:

> We maintain administrative, technical and physical safeguards designed to protect the personal information we collect through our Services against accidental, unlawful destruction, loss, alteration, access, disclosure or use.
>
> Our administrative safeguards include implementing, maintaining, and training employees on company privacy and information security policies and procedures. Our physical and technical safeguards include maintaining physical security policies and standards to protect company systems and data, and a cybersecurity program overseen by executive leadership and the Victoria's Secret & Co. board of directors.

24. Plaintiff and Class members relied on Defendants' implied and expressed promises to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

25. Plaintiff and Class members had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with persons who legitimately needed the information to help Defendants provide assistance or to comply with state and federal statutes and regulations and who could demonstrate to Defendants that they were equipped to protect the PII by having adequate systems and processes in place to safeguard it.

[3] *See* https://www.victoriassecretandco.com/privacy-policy (last visited May 28, 2025).

26. Plaintiff's and Class members' PII is stored on Defendants' network systems.

The Data Breach

27. On May 24, 2025, the Defendants detected unauthorized access on its network as a result of a cybersecurity incident that resulted in the potential exposure of consumers' PII (the "Data Breach").[4] Defendants shut down its website two days later.[5]

28. Defendants have stated that their "ability to maintain the security of customer, associate, third-party and company information" could be compromised. Defendants have "confirmed that hackers accessed the company's IT network, raising fears that customer data was stolen."[6]

29. Defendants failed to take proper measures to safeguard Plaintiff's and Class members' PII from foreseeable cybersecurity threats and allowed criminals to hack their systems and steal Plaintiff's and Class members' sensitive and confidential information.

30. Defendants failed to prevent the data breach because they did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

31. By obtaining, collecting, using and deriving a benefit from Plaintiff's and Class members' PII, Defendants assumed legal and equitable duties to Plaintiff and Class members to protect and safeguard that information from unauthorized access and theft.

32. Defendants facilitated and failed to take reasonable steps to detect, prevent, and mitigate a data breach of its information systems that resulted in the theft of personal information

---

[4] *See* Victoria's Secret's Website Offline Following a Cyberattack, https://securityaffairs.com/178432/hacking/victorias-secrets-website-offline-following-a-cyberattack.html (last visited June 3, 2025).

[5] *See id.*

[6] *See* https://www.pcmag.com/news/victoria-secret-confrims-hack-warns-that-your-data-might-be-at-risk. (last visited June 3, 2025).

of hundreds of thousands, if not more, of current or former customers of the Defendants, including the Plaintiff and Class members.

33. Defendants insufficiently monitored their own systems, and failed to detect the Data Breach which gave the hackers unfettered access to Plaintiff's and Class members' PII.

34. Defendants failed to adequately protect Plaintiff's and Class members' PII—and failed to encrypt or redact this highly sensitive information. Had this information been properly encrypted, the cybercriminals would have made off with only unintelligible data. This unencrypted, unredacted PII was compromised as a direct and proximate result of Defendants' negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class members' PII because of its value in exploiting and stealing Plaintiff's and Class members' identities.

35. Moreover, Defendants have not provided Plaintiff and Class members with timely and adequate notice.

36. The information held by Defendants in their computer systems included Plaintiff's and Class members' unencrypted PII.

37. Plaintiff and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

38. Plaintiff and Class members value, and have taken reasonable steps to maintain, the confidentiality of their PII. Plaintiff and Class members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their PII and demand security to safeguard their PII.

39. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII from involuntary disclosure to third parties. Defendants have a legal duty to keep consumers' PII safe and confidential.

40. Defendants had obligations created by state law, contract, industry standards, and representations made to Plaintiff and Class members, to keep Plaintiff's and Class members' PII confidential and to protect it from unauthorized access and disclosure.

41. Defendants derived a substantial benefit from collecting Plaintiff's and Class members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class members' PII from disclosure.

43. Plaintiff brings this action on behalf of all persons whose PII was compromised because of Defendants' failure to: (i) adequately protect Plaintiff's and Class members' PII; (ii) warn Plaintiff and Class members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence.

44. Defendants disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that Plaintiff's and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even

for internal use. As a result, Plaintiff's and Class members' PII was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

45. Plaintiff and Class members have suffered injury because of Defendants' conduct. These injuries include: (i) lost or diminished value of their PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, unemployment fraud and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

46. Plaintiff and Class members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

Defendants' Personal Information Policy and Promises

47. Defendants made express and implied promises related to its duties and obligations to protect the data they acquired and stored on their system.

48. Defendants' Privacy Policy[7] states that

[7] https://www.victoriassecretandco.com/privacy-policy (last visited May 28, 2025)

> We maintain administrative, technical and physical safeguards designed to protect the personal information we collect through our Services against accidental, unlawful destruction, loss, alteration, access, disclosure or use.
>
> Our administrative safeguards include implementing, maintaining, and training employees on company privacy and information security policies and procedures. Our physical and technical safeguards include maintaining physical security policies and standards to protect company systems and data, and a cybersecurity program overseen by executive leadership and the Victoria's Secret & Co. board of directors.

49. Plaintiff and Class members relied on Defendants' implied and expressed promises to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, such as regularly reviewing activity and system logs to identify potential problems and regularly scanning their network for vulnerabilities, which caused the exposure of PII.

51. The attacker accessed and acquired files in Defendants' computer systems containing Plaintiff's and Class members' PII. Plaintiff's and Class members' PII was accessed and stolen in the Data Breach.

52. Plaintiff further believes that her PII, and the PII of Class members, could be subsequently offered for sale on the dark web following the Data Breach, as PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

53. Plaintiff's and Class members' PII also could also fall into the hands of companies that will use the detailed PII for targeted marketing without Plaintiff's and Class members' approval. Unauthorized individuals can easily access Plaintiff's and Class members' PII.

Data Breaches are Preventable Through Reasonable Security Measures

54. To prevent and detect cyber-attacks and/or ransomware attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or

compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational unit.

55. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[8]

56. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and us strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited May 28, 2025).

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications][9]

57. Given that Defendants were storing Plaintiff's and Class members' sensitive PII, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

58. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach.

Defendants' Storage of Plaintiff's and Class Members' PII

59. As a condition of its relationships with Plaintiff and Class members, Defendants required that Plaintiff and Class members entrust Defendants with highly sensitive and confidential PII. Plaintiff and Class members provided their PII with the reasonable expectation and mutual understanding that Defendants would safeguard the PII against foreseeable threats.

60. Defendants, in turn, stored that information in the part of Defendants' computer and information system that was ultimately affected by the Data Breach.

61. By obtaining, collecting, and storing Plaintiff's and Class members' PII,

[9] See Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited May 28, 2025).

Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

62. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

63. Defendants could have prevented this targeted Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class members' PII.

64. Upon information and belief, Defendants made promises to Plaintiff and Class members to maintain and protect PII, demonstrating an understanding of the importance of securing PII.

Defendants Knew or Should Have Known of Their Susceptibility to Cyber Attacks

65. Data thieves regularly target governmental agencies due to the highly sensitive information that they collect and store. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

66. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendants, preceding the date of the Data Breach.

67. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S.

68. In 2022, 1,802 data breaches occurred, resulting in over 422,000,000 sensitive

records being exposed.[10] The over 422,000,000 records being exposed in 2022 represents a substantial increase from 2021 when 293,927,708 sensitive records were exposed in 1,862 data breaches.

69. In light of recent high profile data breaches at other industry leading companies, including MOVEIt (17.5 million records, June 2023), LastPass/GoTo Technologies (30 million records, August 2022), Neopets (69 million records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 million records, July 2022), Cash App (8.2 million users, April 2022), LinkedIn (700 million records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII they collected and maintained would be targeted by cybercriminals.

70. Additionally, as governmental agencies became more dependent on computer systems to run their processes,[11] (*e.g.*, working remotely because of the Covid-19 pandemic), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[12]

71. As a custodian of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members, and of the foreseeable

---

[10] *See* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited May 28, 2025). *Id.; see also* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6. (last visited May 28, 2025).

[11] *See* https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited May 28, 2025).

[12] *See* https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited May 28, 2025).

consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class members as a result of a breach.

72. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class members' PII from being compromised.

73. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class members' PII and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members because of a breach.

74. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for Plaintiff's and Class members' PII.

76. The ramifications of Defendants' failure to keep secure Plaintiff's and Class members' PII are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

77. The breadth of data believed to have been compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

78. Defendants knew, or should have known, the importance of safeguarding the PII

entrusted to them by Plaintiff and Class members and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

The Value of Personal Identifiable Information

79. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

80. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[15] For example, Personal Information can be sold at a price ranging from $40 to $200.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.23.[17]

81. For example, Social Security numbers, which may have been compromised for

[13] 17 C.F.R. § 248.201 (2013).
[14] *Id.*
[15] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 28, 2025).
[16] Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-thedark-web/ (last visited May 28, 2025).
[17] In the Dark, VPN Overview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 28., 2025).

Plaintiff and Class members, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot a lot of problems.[18]

82. What's more, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

83. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

84. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of

---

[18] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 28, 2025).

[19] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworryingabout-identity-theft (last visited May 28, 2025).

identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as names, addresses, email addresses, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

85. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

86. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

87. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

88. Plaintiff and Class members now face years of constant surveillance of their

[20] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 28, 2025).

[21] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited May 28, 2025).

financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendants Failed to Comply with Industry Standards

89. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that, at a minimum, should be implemented by organizations in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; and backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard in government operations include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including by failing to train staff.

92. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards in the industry, and upon information and belief, Defendants failed to comply with at least one—or all––of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Damages

94. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class members has materialized and is imminent, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

95. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information, precisely as they have done here. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

96. Because a person's identity is akin to a puzzle with multiple data points, the more

accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

98. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[22] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

99. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that their PII was compromised, as here, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to

[22] *What is the Dark Web?*, Experian available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited May 29, 2025).
[23] *Id.*

spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

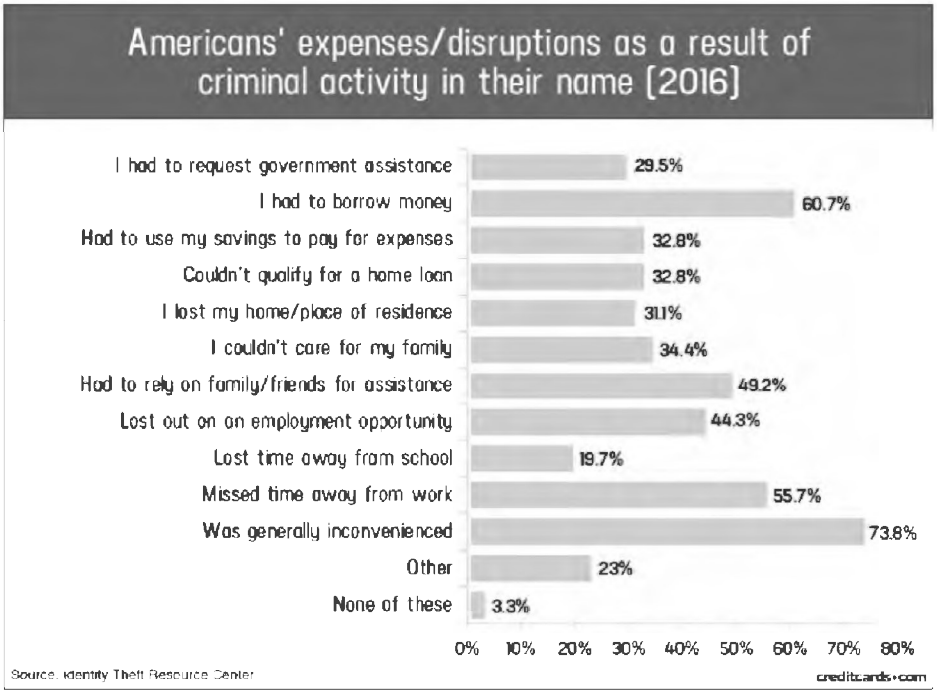
100. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must, as the Notice encourages them to do, monitor their financial accounts for many years to mitigate the risk of identity theft.

101. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such contacting financial institutions, closing or modifying financial accounts, signing up for credit and identity theft monitoring insurance, and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

102. Plaintiff's and Class members' mitigation efforts are also consistent with the steps that the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

103. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[24]

[24] Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited May 28, 2025).



104. According to the Electronic Privacy Information Center:

> Identity theft is an enormous problem for consumers. The Federal Trade Commission reported 399, 225 cases of identity theft in the United States in 2016. Of that number, 29% involved the use of personal data to commit tax fraud. More than 32% reported that their data was used to commit credit card fraud, up sharply from 16% in 2015. A 2015 report from the Department of Justice found that 86% of the victims of identity theft experienced the fraudulent use of existing account information, such as credit card or bank account information. The same report estimated the cost to the U.S. economy at $15.4 billion.[25]

105. PII is a valuable property right.[26] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

106. An active and robust legitimate marketplace for PII also exists. In 2019, the data

[25] See https://archive.epic.org/privacy/data-breach/equifax/ (last visited May 29, 2025).
[26] See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last visited May 29, 2025).

brokering industry was worth roughly $200 billion.[27] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[28]

107. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

108. To date, Defendants have nothing to provide Plaintiff and Class members with relief for the damages they have suffered as a result of the Data Breach.

109. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

110. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

111. The retail cost of credit monitoring and identity theft monitoring can cost $200 or

[27] See https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited May 29, 2025).
[28] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 29, 2025).

more a year per Class member. This is a reasonable and necessary cost to protect Class members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear but for Defendants' failure to safeguard their PII.

112. Furthermore, Defendants' poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to provide their PII, which was a condition precedent to obtain services, and paying Defendants for their services, Plaintiff as a consumer understands and expected that she was, in part, paying for services and data security to protect the PII required to be collected from her.

113. Defendants did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendants.

114. Plaintiff and Class members have been damaged by the compromise and exfiltration of their PII in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

115. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

116. Further, Plaintiff and Class members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees,

credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

117. In addition, Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach.

118. Plaintiff and Class members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

119. Defendants' delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendants knew of the breach and did not formally notify victims. This delay increases the injuries to Plaintiff and Class.

FACTS RELEVANT TO PLAINTIFF SUSAN WARDLE-BURKE

120. Plaintiff is a Victoria's Secret customer and credit card holder. Upon information and belief prior to the Data Breach, the Defendants maintained Plaintiff's PII in its systems.

121. Prior to the Data Breach, Plaintiff was very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

122. Plaintiff learned of the Data Breach by reviewing media reports of the website outage late in the day on May 27, 2025. Upon reviewing the media reports, Plaintiff spent time reviewing credit reports, reviewing various credit alerts received by text and email, checking her

financial information, and dealing with increased spam text messages and emails.

123. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach, and Plaintiff has anxiety and increased concerns for the loss of her privacy.

124. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

125. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

126. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

127. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

128. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

129. As a result of the Data Breach, Plaintiff and the other Class members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

130. Plaintiff and the other members of the Class have suffered and will suffer actual

injury as a direct result of the Data Breach, including in the form of out-of-pocket expenses and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendants;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be canceled; and

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

131. Plaintiff and the other Class members have an interest in ensuring that Defendants implement reasonable security measures and safeguards to maintain the integrity and confidentiality of their financial and personally identifiable information, including making sure

that the storage of data or documents containing personal and financial information is not accessible by unauthorized persons and that access to such data is sufficiently protected.

132. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and the other Class members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

133. **Class Definition**: Plaintiff brings this action pursuant to Civ. R. 23, on behalf of a class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party because of the data breach reported by Defendants during May 2025 (the "Class").

Excluded from the Class are Defendants and their subsidiaries and affiliates; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and their/her immediate family and court staff.

134. **Numerosity**: Upon information and belief, based on Victoria's Secret being a large retailer, the class is believed to be comprised of hundreds of thousands of Class members. Thus, the Class is so numerous that joinder of all members is impracticable. Class members can easily be identified through Defendants' records, or by other means.

135. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiff and the other Class members, which predominate over any individual issues, including:

A. Whether Defendants adequately protected Plaintiff's and other Class members' PII;

B. Whether Defendants stored Plaintiff's and other Class members' PII without implementing reasonably adequate security to protect the information;

C. Whether Defendants adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to Plaintiff's and other Class members' PII;

D. Whether Defendants properly trained and supervised employees to protect Plaintiff's and other Class members' PII;

E. Whether Defendants promptly notified Plaintiff and the other members of the Class of the Data Breach;

F. Whether Defendants owed a duty to Plaintiff and the other members of the Class to safeguard and protect their PII;

G. Whether Defendants breached their duty to Plaintiff and the other members of the Class to safeguard and protect their PII;

H. Whether Defendants breached their duty to Plaintiff and the other members of the Class by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect Plaintiff's and other Class members' PII;

I. Whether Defendants' conduct constituted a breach of contract with Plaintiff and Class members; and

J. Whether Defendants are liable for the damage suffered by Plaintiff and the other members of the Class as a result of the Data Breach.

136. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. All claims are based on the same legal and factual issues. Plaintiff and each of the other Class members provided their PII to Defendants, and the information was compromised in the Data Breach. Defendants' conduct was uniform with respect to all Class members.

137. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to the Class, and Defendants have no defense unique to Plaintiff.

138. **Superiority**: A class action is superior to other available methods for the fair and

efficient adjudication of this controversy. The expense and burden of individual litigation would make it impractical or impossible for members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiff's claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

139. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

140. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and other Class members' personal and financial information of and the importance of adequate security. Defendants were aware of numerous, well-publicized data breaches that exposed the personal, financial, or health information of individuals. Defendants were also aware of the risk presented by groups, like the hackers, from the FBI's publications.

141. Defendants have a common law duty to prevent foreseeable harm to those who entrusted their PII to Defendants. This duty existed because Plaintiff and the other Class members were foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiff's and the other Class members' PII would not be accessible by unauthorized persons.

142. Defendants had a special relationship with Plaintiff and the other Class members. Defendants were entrusted with Plaintiff's and the other Class members' PII, and Defendants were in a position to protect their PII from unauthorized access and activity.

143. Defendants had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' PII in their possession so that the PII would not come within the possession, access, or control of unauthorized persons.

144. More specifically, the duties of Defendants included, among other things, the duty to:

A. Adopt, implement, and maintain policies, procedures, and security measures for protecting Plaintiff's and the other Class members' PII, including policies, procedures, and security measures;

B. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing Plaintiff's and other Class members' PII with entities that failed to adopt, implement, and maintain policies, procedures, and security measures;

C. Adopt, implement, and maintain reasonable policies and procedures to ensure that Plaintiff's and the other Class members' PII is disclosed only with authorized persons who have adopted, implemented, and maintained policies, procedures, and security measures;

D. Properly train their employees to protect documents containing Plaintiff's and the other Class members' PII; and

E. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly repel breaches to the security of their systems.

145. In violation of their duties, Defendants failed to exercise due care in the following ways, which caused the Data Breach:

A. Failed to update both software and applications with the latest patches as soon as possible to protect them from vulnerabilities;

B. Failed to ensure that backups are secure and disconnected from the network at the conclusion of each backup session;

C. Failed to monitor inbound and outbound network traffic, with alerts for data exfiltration in place;

D. Failed to implement the principle of least privilege for file, directory, and network share permissions;

E. Failed to consistently enforce security policies aimed at protecting Plaintiff's and Class members' PII; and

F. Failed to implement processes to detect data breaches, security incidents, or intrusions quickly.

146. Defendants breached the foregoing duties and failed to exercise reasonable care in the ways described above in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and the other Class members' PII in their possession, custody, and care.

147. Defendants acted with reckless disregard for the security of Plaintiff's and other Class members' PII because Defendants knew or should have known that their data security practices were not adequate to safeguard the PII that they collected and stored.

148. Defendants acted with reckless disregard for Plaintiff's and other Class members' rights by failing to promptly detect the Data Breach and provide prompt notice so that Plaintiff and the other Class members could take measures to protect themselves from damages caused by the unauthorized access of the accounts compromised in the Data Breach and loss of services while the Data Breach occurred.

149. As a direct and proximate result of Defendants' misconduct, Plaintiff and Class members sustained damages or are likely to sustain damages, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred should identity theft occur; (e) loss of time incurred should identity theft occur; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance; and (j) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

150. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

151. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendants, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

152. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

153. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

154. Class members are consumers within the class of persons that Section 5 of the FTC Act was intended to protect.

155. Moreover, the harm that has occurred is the type of harm that the FTC Act intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm Plaintiff and Class members suffered.

156. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, Plaintiff's and Class members' PII of would not have been compromised.

157. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class members' PII and the harm, or risk of imminent

harm Plaintiff and the Class suffered. Plaintiff's and Class members' PII was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

158. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

159. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

160. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

161. Plaintiff and Class members are entitled to compensatory and consequential

damages suffered because of the Data Breach.

162. Defendants' negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class members in an unsafe and insecure manner.

163. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

164. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

165. Plaintiff and the Class members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their information had been breached and compromised.

166. Plaintiff and Class members were required to deliver, and delivered, their PII to Defendants as part of the process of obtaining services provided by Defendants.

167. Defendants accepted possession of Plaintiff's and Class members' PII for the purpose of providing services to Plaintiff and Class members.

168. In accepting such information for services, Plaintiff and the other Class members entered into an implied contract with Defendants in which Defendants became obligated to reasonably safeguard Plaintiff's and the other Class members' PII.

169. In delivering their PII to Defendants and receiving services, Plaintiff and Class

members intended and understood that Defendants would adequately safeguard the data as part of that service.

170. In its privacy and security policies as explained on its website, Defendants expressly promised to Plaintiff and Class members that they would only disclose protected information and other PII under certain circumstances, none of which related to a Data Breach as occurred in this matter.

171. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; and (6) other steps to protect against foreseeable data breaches.

172. Plaintiff and Class members would not have entrusted their PII to Defendants in the absence of such an implied contract.

173. Had Defendants disclosed to Plaintiff and Class members that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class members would not have provided their PII to Defendants.

174. Defendants recognized that Plaintiff's and Class members' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the other Class members.

175. Plaintiff and the other Class members fully performed their obligations under the implied contracts with Defendants.

176. Defendants breached the implied contract with Plaintiff and the other Class members by failing to take reasonable measures to safeguard their data as described herein.

177. As a direct and proximate result of Defendants' misconduct, Plaintiff and Class members have sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs should identity theft occur; (e) loss of time incurred should identity theft occur; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance; and (j) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

178. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

179. In light of the special relationship between Defendants and Plaintiff and Class members, whereby Defendants became guardian of Plaintiff's and Class members' PII, Defendants became a fiduciary, by their undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members: (1) for the safeguarding of Plaintiff's and Class members' PII; (2) to timely notify Plaintiff and Class members of the Data Breach with proper disclosures; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

180. Defendants have a fiduciary duty to act for Plaintiff's and Class members' benefit

upon matters within the scope of Defendants' relationship with Plaintiff and Class members to keep their PII secure.

181. Defendants breached their fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

182. Defendants breached their fiduciary duties to Plaintiff and Class members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff's and Class members' PII.

183. Defendants breached their fiduciary duties owed to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

184. Defendants breached their fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PII.

185. As a direct and proximate result of Defendants' misconduct, Plaintiff and Class members sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs should identity theft occur; (e) loss of time should identity theft occur; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance; and (j) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

186. Plaintiff and Class members are entitled to compensatory, consequential, and

nominal damages suffered as a result of the Data Breach.

187. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT V
Invasion of Privacy
(Intrusion Upon Seclusion)
(On Behalf of Plaintiff and the Class)

188. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

189. Plaintiff and Class members had a reasonable expectation of privacy in the PII.

190. As a result of Defendants' conduct, Plaintiff's and Class members' PII was publicly disclosed, which necessarily includes matters concerning their private life such as their PII.

191. Plaintiff's and Class members' PII is not of legitimate public concern and should remain private.

192. By knowingly failing to keep Plaintiff's and Class members' PII safe, and by knowingly misusing said information, Defendants negligently, recklessly, and intentionally invaded Plaintiff's and Class members' privacy by intruding into Plaintiff's and Class members' private affairs, without approval, in a manner that would be highly offensive and objectionable to a person of ordinary sensibilities.

193. Defendants knew that an ordinary person in Plaintiff's and Class members' position would consider Defendants' negligent, reckless, and intentional actions highly offensive and objectionable.

194. Such an intrusion into Plaintiff's and Class members' private affairs of is likely to

cause outrage, shame, and mental suffering because the PII disclosed includes sensitive personal information that allow third parties to commit fraud and identity theft.

195. Defendants invaded Plaintiff's and Class members' right to privacy of, and intruded into Plaintiff's and Class members' private lives, by negligently, recklessly, and intentionally misusing their PII without their informed, voluntary, affirmative, and clear consent.

196. Defendants intentionally concealed from Plaintiff and Class members an incident that misused their PII without their informed, voluntary, affirmative, and clear consent.

197. As a proximate result of such intentional misuse, the reasonable expectations of privacy that Plaintiff and Class members have in their PII was unduly frustrated and thwarted.

198. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and Class members' protected privacy concerns, caused anguish and suffering such that a person with ordinary sensibilities would consider Defendants' intentional actions or inaction highly offensive and objectionable.

199. In failing to protect Plaintiff's and Class members' PII, and in negligently, recklessly, and intentionally misusing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class members' rights of to have such information kept secure, confidential, and private.

200. As a direct and proximate result of Defendants' misconduct, Plaintiff and Class members sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs should identity theft occur; (e) loss of time should identity theft occur; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution

of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance; and (j) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

201. Plaintiff and Class members are entitled to compensatory, consequential, punitive, and nominal damages suffered because of the Data Breach.

202. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

203. Plaintiff realleges and incorporates by reference all preceding allegations, as if fully set forth herein.

204. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

205. Plaintiff and Class members conferred a benefit on Defendants. Specifically, Plaintiff and Class members purchased merchandise that generated revenue for Defendants, as well as used a store credit card, for which Defendants benefitted from the interest charged on outstanding balances. In exchange, Defendants should have protected Plaintiff's and Class members' PII with adequate data security.

206. Defendants knew that Plaintiff and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendants

profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

207. Defendants failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

208. Defendants acquired the PII through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

209. If Plaintiff and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants or purchased merchandise from Victoria's Secret.

210. Plaintiff and Class members have no adequate remedy at law.

211. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their PII.

212. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

213. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

214. Plaintiff and Class members are entitled to restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

215. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Susan Wardle-Burke, individually, and on behalf of all others similarly situated, respectfully requests that judgment be entered in favor of the Class and against Defendants as follows:

A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certify the Class defined herein;

B. That the Court appoint Plaintiff as representative of the Class;

C. That the Court appoint Plaintiff's counsel as counsel for the Class;

D. That the Court enter judgment in favor of Plaintiff and the Class and against Defendants;

E. That the Court award Plaintiff and the other Class members actual damages and all other forms of available relief, as applicable;

F. That the Court award Plaintiff and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

G. That the Court enter an injunction requiring Defendants to adopt, implement, and maintain adequate security measures to protect their customers' personal and financial information; and

H. Grant all such further and other relief as the Court deems just and appropriate.

JURY TRIAL DEMANDED

Plaintiff SUSAN WARDLE-BURKE hereby demands a trial by jury on all claims so triable.

Plaintiff SUSAN WARDLE-BURKE, individually and on behalf of all others similarly situated,

/s/ Brian D. Flick
Brian D Flick (OH 0081605)
Marc E. Dann (OH 0039425)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
firm@attorneyzim.com

**Pro Hac Vice* Motion to be submitted

Counsel for Plaintiff and the Proposed Class